IN THE CLAIMS

1. (Currently Amended) A computer-implemented method, comprising:

retrieving a first key from a secure store associated with a firmware within a platform, the firmware including an initialization table for initializing the platform, wherein the initialization table comprises one or more initialization segments that are individually executable; ~~and~~

verifying the initialization table using the first key retrieved from the secure store during an initialization of the platform;

retrieving a second key from the secure store; and

verifying at least one initialization segment using the second key retrieved from the secure store.

2. (Cancelled)

3. (Currently Amended) The method of ~~claim 2~~claim 1, wherein the at least one initialization segment is signed using the second key prior to being stored in the firmware.

4. (Currently Amended) The method of claim 1~~claim 2~~, further comprising examining the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the verification is performed only if the at least one initialization segment includes the code to be dispatched.

5. (Currently Amended) The method of claim 4, further comprising:

determining whether the verification of the at least one initialization segment is performed successfully; and executing the code dispatched from the at least one initialization segment if the verification of the at least one initialization segment is performed successfully.

6. (Original) The method of claim 5, further comprising resetting the platform if the verification is performed unsuccessfully.

7. (Currently Amended) The method of claim 1~~claim 2~~, further comprising executing the at least one initialization segment without performing the verification, if the at least one initialization segment does not include the code to be dispatched.

8. (Original) The method of claim 1, wherein the initialization of the platform is performed during a resume process of the platform, and wherein the first and second keys are generated, and the initialization table and the at least one initialization segment are signed during a boot process of the platform.

9. (Currently Amended) A machine-readable storage medium having executable code to cause a machine to perform a method, the method comprising:

retrieving a first key from a secure store of a firmware within a platform, the firmware including an initialization table for initializing the platform, wherein the initialization table comprises one or more initialization segments that are individually executable; ~~and~~

verifying the initialization table using the first key retrieved from the secure store during an initialization of the platform;

retrieving a second key from the secure store; and

verifying at least one initialization segment using the second key retrieved from the secure store.

10. (Cancelled)

11. (Currently Amended) The machine-readable storage medium of ~~claim 10~~claim 9, wherein the method further comprises examining the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the verification is performed only if the at least one initialization segment includes the code to be dispatched.

12. (Currently Amended) The machine-readable storage medium of claim 11, further comprising:

determining whether the verification is performed successfully; and

executing the code dispatched from the at least one initialization segment if the verification is performed successfully.

13. (Currently Amended) A data processing system, comprising:

a processor;

a memory coupled to the processor to store an initialization table~~ for initializing the data processing system~~, the memory including a secure store; and

a process, when executed from the memory, causes the processor to

retrieve a first key from the secure store, ~~and~~

verify the initialization table using the first key retrieved from the secure store during an initialization of the data processing system, wherein the initialization table comprises one or more initialization segments that are individually executable,

retrieve a second key from the secure store, and

verify at least one initialization segment using the second key retrieved from the secure store.

14. (Cancelled)

15. (Currently Amended) The data processing system of ~~claim 14~~claim 13, wherein the process further causes the processor to examine the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched, wherein the verification is performed only if the at least one initialization segment includes the code to be dispatched.

16. (Currently Amended) A computer-implemented method, comprising:

generating a first key to sign an initialization table of a firmware in a platform, the initialization table being used to initialize the platform, wherein the initialization table comprises one or more initialization segments that are individually executable;

signing the initialization table using the first key;

storing the first key in a secure store of the firmware; ~~and~~

generating a second key;

signing at least one initialization segment of the initialization table using the second key;

storing the second key in the secure store; and

locking the secure store after the first key ~~is~~ and the second key are stored in the secure store.

17. (Cancelled)

18. (Currently Amended) The method of ~~claim 17~~claim 16, further comprising examining the at least one initialization segment to determine whether the at least one initialization

segment includes code to be dispatched, wherein the signing operations using the second key is performed only if the at least one initialization segment includes the code to be dispatched.

19. (Original) The method of claim 16, wherein the first and second keys are generated, and the initialization table and the at least one initialization segment are signed during a boot process of the platform.

20. (Currently Amended) A machine-readable storage medium having executable code to cause a machine to perform a method, the method comprising:

generating a first key to sign an initialization table of a firmware in a platform, the initialization table being used to initialize the platform, wherein the initialization table comprises one or more initialization segments that are individually executable;

signing the initialization table using the first key;

storing the first key in a secure store of the firmware; ~~and~~

generating a second key;

signing at least one initialization segment of the initialization table using the second key;

storing the second key in the secure store; and

locking the secure store after the first key ~~is~~ and the second key are stored in the secure store.

21. (Cancelled)

22. (Currently Amended) The machine-readable storage medium of ~~claim 21~~claim 20, wherein the method further comprises examining the at least one initialization segment

to determine whether the at least one initialization segment includes code to be dispatched, wherein the signing operation using the second key is performed only if the at least one initialization segment includes the code to be dispatched.

23. (Currently Amended) A data processing system, comprising:

a processor;

a memory coupled to the processor to store an initialization table~~ for initializing the data processing system~~, the memory including a secure store; and

a process, when executed from the memory, causes the processor to

generate a first key to sign the initialization table, wherein the initialization table comprises one or more initialization segments that are individually executable,

sign the initialization table using the first key,

store the first key in the secure store, ~~and~~

generate a second key,

sign at least one initialization segment of the initialization table using the second key,

store the second key in the secure store, and

lock the secure store after the first key ~~is~~ and the second key are stored in the secure store.

24. (Cancelled)

25. (Currently Amended) The data processing system of ~~claim 24~~claim 23, wherein the process further causes the processor to examine the at least one initialization segment to determine whether the at least one initialization segment includes code to be dispatched,

wherein the signing operation using the second key is performed only if the at least one initialization segment includes the code to be dispatched.

26. – 30. (Cancelled)